Виявлення невидимих загроз: Аналіз даних на основі штучного інтелекту дозволяє виявляти навіть ті кіберзагрози, які можуть діяти в режимі хамелеона, намагаючись залишитися непоміченими.

Системи виявлення і відновлення (EDR): Системи штучного інтелекту сприяють створенню розширених систем виявлення і відновлення, які не лише виявляють загрози, але й автоматично вживають заходів для їхнього усунення та відновлення.

Ці аспекти демонструють, як системи штучного інтелекту стають ключовим інструментом для ефективного виявлення та боротьби з кіберзагрозами.

Література

1. Milov O. et al. Development of the space-time structure of the methodology for modeling the behavior of antagonistic agents of the security system. Eastern-European Journal of Enterprise Technologies. 2020. Т. 6. №. 2. PP. 30-32. DOI: 10.15587/1729-4061.2020.218660 URL: https://www.scopus.com /record/display.uri?eid=2-s2.0-85104142498&origin=resultslist&sort=plf-f

2. Синиціна Ю.П., Станіна О.Д. (2021) Обґрунтування актуальності цифрової комунікації закладів вищої освіти: міжнар. колект. моногр. «Digital Economy and Digital Society» III Міжнародна конференція (28–29 травня 2021 р.) Katowice, University of Technology, Poland,. 10 с. URL: https://isg-konf.com/wp-content/uploads/2021/12/Monograph/Monograph-USA-Technical-2021-III-isg-konf.pdf

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ DECEPTION У БОРОТЬБІ З КІБЕРЗАГРОЗАМИ

Лунгол Ольга Миколаївна
кандидат педагогічних наук, доцент, доцент кафедри
оперативно-розшукової діяльності та інформаційної безпек
факультету №3 підготовки фахівців для підрозділів кримінальної поліції
Донецького державного університету внутрішніх справ
Агішева Анна Володимирівна
викладач інформатики Кропивницького вищого професійного училища

В епоху, коли кіберзагрози стають все більш виразними та вибагливими, використання технології Deception стає важливим елементом ефективної кібербезпеки. Ця інноваційна стратегія займає важливе місце у глобальній війні проти кіберзлочинців, забезпечуючи активний та інтелектуальний захист інформаційних ресурсів. Технологія Deception дозволяє створювати штучні об’єкти та фальшиві елементи в системі, що дозволяє дієво виявляти та активно протидіяти кіберзагрозам. Зловмисники, які намагаються провести цілеспрямовані атаки в мережі, змушені витрачати час та ресурси на штучно створені фіктивні об’єкти, що значно ускладнює їх діяльність та зменшує ймовірність успіху. Створені фальшиві об’єкти відволікають увагу зловмисників, змушуючи їх зосередитися на неважливих або неправдивих елементах системи, що надає більше часу для виявлення та реагування на потенційні загрози безпеці інформаційних ресурсів.

Однією з ключових переваг технології Deception є її здатність виявляти атаки на ранніх етапах. Це дозволяє оперативно реагувати та запобігати вторгненням в систему, зменшуючи час, протягом якого зловмисники можуть завдати шкоди.

Одна з основних проблем в кібербезпеці полягає у тому, що системи можуть надто часто спрацьовувати на помилкові загрози, що призводить до зайвої витрати ресурсів, або, навпаки, ігнорування реальних атак. Технологія Deception спрямована на зменшення помилок виявлення атак, відомих як «false positives». Такі «false positives» можуть виникати з різних причин, включаючи помилкові сигнали від захисних систем або проблеми з конфігурацією детекторів загроз. Технологія Deception вирішує цю проблему, надаючи системі фальшиві об’єкти, які призначені привертати увагу потенційних зловмисників та імітувати діяльність реальних елементів мережі. Таким чином, технологія Deception створює контрольовані умови для виявлення атак, не спричиняючи неважливих спрацювань на реальних елементах мережі. Наявність фальшивих об’єктів також створює психологічний

тиск на зловмисників, змушуючи їх перейматися великою ймовірністю повторної невдачі та ризиком розкриття.

Загальний алгоритм роботи технології Deception включає наступні кроки:

1. Створення фальшивих об’єктів (захисна система створює фальшиві ресурси, такі як файли, сервери, мережеві вузли або інші цифрові об’єкти. Ці об’єкти максимально схожі на реальні елементи мережі).
2. Розгортання фальшивих об’єктів (фальшиві об’єкти розгортаються в різних частинах мережі чи інфраструктури компанії. Розташування та характеристики фальшивих об’єктів можуть бути стратегічно обрані, щоб привернути увагу зловмисників).
3. Моніторинг та виявлення (фальшиві об’єкти активно моніторяться на наявність неправомірної взаємодії. Захисна система аналізує взаємодію та виявляє аномалії, що можуть свідчити про злочинну діяльність)
4. Взаємодія зловмисників (якщо зловмисники спробують взаємодіяти з фальшивим об’єктом, система фіксує цю діяльність. Відповідно до виявлених загроз, система може вжити певних заходів, таких як блокування зловмисників, реєстрація їхньої діяльності чи сповіщення адміністраторів безпеки).
5. Збір інтелектуальної інформації (в процесі взаємодії із зловмисниками фальшиві об’єкти можуть збирати інформацію про методи атак та інші аспекти злочинної діяльності).
6. Аналіз та вдосконалення (отримана інформація використовується для вдосконалення та адаптації технології Deception до нових видів загроз).

Технологія Deception може бути порівняна з іншими подібними технологіями, такими як Honeypots та Honeynets, які також використовуються для виявлення та обмеження кіберзагроз. Технологія Deception має кілька переваг в порівнянні з іншими подібними технологіями, серед яких ми виділяємо: гнучкість і розширюваність (Deception дозволяє створювати фальшиві об’єкти в різних частинах інфраструктури, що надає значну гнучкість в розгортанні, можливість використовувати Deception для захисту різноманітних ресурсів, включаючи файли, дані, мережі та інші елементи); точність виявлення (Deception орієнтована на точне виявлення атак, забезпечуючи мінімізацію помилок); мінімізація ризиків; проактивний підхід (Deception дозволяє створювати реалістичні хибні об’єкти та стимулювати проведення атак, намагаючись привернути увагу зловмисників, що дозволяє більш ефективно виявляти потенційні загрози); захист від внутрішніх загроз (Deception може застосовуватися для виявлення навіть внутрішніх загроз, таких як неавторизований доступ в мережу власних співробітників або витоків конфіденційної інформації); легке впровадження (технологія Deception може бути легше впроваджена в систему в порівнянні з деякими іншими альтернативами).

Загалом, технологія Deception створює докладну ілюзію реальності для зловмисників і надає ефективний засіб виявлення та захисту від кіберзагроз. У світі постійно зростаючих кіберзагроз використання технології Deception стає стратегічною необхідністю для забезпечення повноцінного захисту від кіберзлочинців та збереження цілісності інформаційних ресурсів.

Література:

1. Шаєц Є., Лунгол О. Використання ханіпотів для виявлення мережевих атак. Інформаційна безпека та інформаційні технології: IV Міжнар. наук.-практ. конф. (м. Львів, 30 листопада 2022 р.). Львів : Растр-7, 2022. С. 93–95.
2. Технологія обману. Що таке Deception і як обманюють хакерів. 10Guards. Режим доступу: https://10guards.com/ua/articles/deception-technology-and-how-it-can-trap-cyberattackers/ (Дата звернення: 09.11.2023).